PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-092605

(43)Date of publication of application : 28.03.2003

(51)Int.Cl. H04L 12/58

(21)Application number : 2001-283389

(22)Date of filing : 18.09.2001

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>

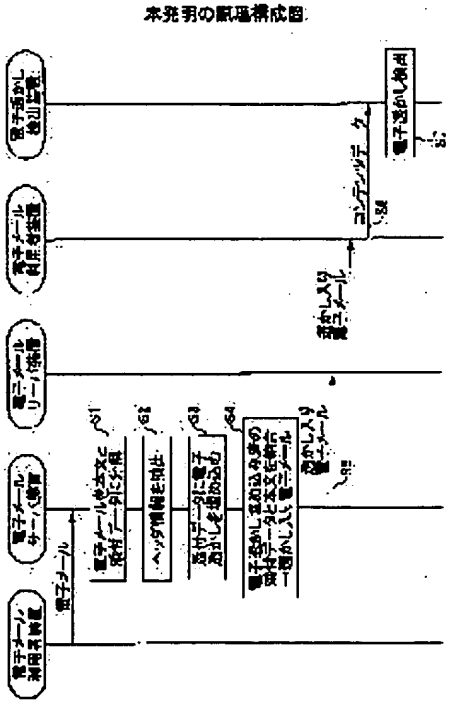
(72)Inventor : NAKAMURA TAKAO
KIMURA TSUKASA

(54) CONTENTS PROTECTION METHOD AND SYSTEM, CONTENTS PROTECTION PROGRAM AND STORAGE MEDIUM WITH THE CONTENTS PROTECTION PROGRAM STORED

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent illegal distribution by an electronic mail user registered in an electronic mail server apparatus and illegal distribution by users receiving contents data by electronic mail in distributing contents by using electronic mail.

SOLUTION: An electronic mail server of this invention extracts header information sent from a user apparatus, embeds an electronic watermark into attached data by using an electronic watermark technology, transfers the electronic mail with the electronic watermark embedded thereto to other electronic mail server apparatus, and electromagnetic detection apparatus receives contents data sent from the user apparatus via the electronic mail server to detect the electronic watermark.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of

rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[The technical field to which invention belongs] this invention relates to the storage which stored the contents protection method, the system, the contents protection program, and the contents protection program, and relates to the storage which stored the contents protection method, the system, contents protection program, and contents protection program for protecting the copyright in the digital contents distribution on a network especially.
[0002]
[Description of the Prior Art] The contents circulation on a network is becoming active with the spread of information networks, such as the Internet, and digitization of contents. An E-mail is in some which are widely used as means of communications using the network. As for an E-mail user, in an E-mail, it is common to register oneself into the electronic mail server equipment which ISP (Internet service provider) manages, and to transmit and receive mail.
[0003]
[Problem(s) to be Solved by the Invention] However, there is a problem that literary piracy will also be easy with the property which digital contents have. That is, once it gets digital data, anyone can perform the copy which does not have degradation easily any number of times, and since oneself may become the addresser of data, it will enable the addressee of contents data further to distribute a copy in the form which the transmitting person (copyright person) of the original contents data does not mean.

[0004] It is general means of communications. An E-mail is communication of 1 to 1 or one-pair ** fundamentally, and, generally the exchange of an E-mail is not noticed other than a transceiver person. Although the responsibility may be imposed on ISP which is the manager of electronic mail server equipment when distribution of the inaccurate contents using the E-mail is performed, it is difficult to specify who [of the E-mail users whom oneself manages as mentioned above] performed injustice. When the employee makes external extra sensitive information reveal in a company etc., using an E-mail as same case, there is a problem that it is difficult to determine the criminal.
[0005] Moreover, considering the case where the owner (copyright person) of contents data performs contents data distribution using an E-mail, there is a problem that it is difficult for the user of the distribution place of contents data to prevent unjust distribution of the data acquisition backward above.

[0006] this invention was made in view of the above-mentioned point, and in the contents distribution using the E-mail, it aims at offering the storage which stored the contents protection method which can prevent unjust distribution of the user who received contents data by the E-mail, the system, the contents protection program, and the contents protection program while it prevents the unjust distribution by the E-mail user registered into a certain electronic mail server equipment.
[0007]
[Means for Solving the Problem] Drawing 1 is drawing for explaining the principle of this invention.
[0008] In the contents protection method for this invention (claim 1) preventing unjust distribution of contents in the case of the contents distribution using the network communication containing an E-mail In electronic mail server equipment, the E-mail sent from E-mail user equipment is decomposed into the E-mail text and appending data (Step 1). The header information described by the header unit of an E-mail is extracted (Step 2). Digital watermarking is embedded in appending data using header information and digital-watermarking technology (Step 3). Combine with the E-mail text, space the appending data which embedded digital watermarking, and an entering E-mail is created (Step 4). Space, transmit an entering E-mail to another electronic mail server equipment by the usual delivery method (Step 5), and it sets to digital-watermarking detection equipment. Contents data are received through electronic mail server equipment from the E-mail user equipment of the receiving side which spaced and received the entering E-mail (Step 6). When digital watermarking is detected from contents data and digital watermarking is detected, the information currently embedded is outputted as information about unjust transmission (Step 7). this invention (claim 2) acquires the message ID which shows an E-mail to a meaning in electronic mail server equipment, it embedded message ID in appending data using digital-watermarking technology, made message ID and header information the group, registered them into the header information database, considers that the information outputted by detection processing of digital watermarking is message ID in digital-watermarking detection equipment, and acquires the E-mail to which it corresponds in a header information database
[0009] When, as for this invention (claim 3), electronic mail server equipment has the function of digital-watermarking detection equipment, Receive the E-mail where digital watermarking was embedded, and an E-mail is decomposed into the E-mail text and appending data. When the header information containing the destination e-mail address described by the header unit of an E-mail is acquired, digital watermarking from appending data is detected and detection of digital watermarking is successful When the justification of an E-mail is checked using a consistency check or the predetermined conditions of the destination e-mail address described by the destination e-mail address currently embedded and header information and justification cannot be checked, processing for preventing injustice is performed.
[0010] Drawing 2 is the principle block diagram of this invention.
[0011] this invention (claim 4) is a contents protection system for preventing unjust distribution of contents in the case of the contents distribution using the network communication containing an E-mail. An appending data decomposition means 21 to decompose into the E-mail text and appending data the E-mail sent from E-mail user equipment 10, A header information acquisition means 22 to extract the header information described by the header unit of an E-mail, The digital-watermarking embedded means 23 which embeds header information as digital watermarking in

appending data using digital-watermarking technology, An appending data-coupling means 24 to combine with the E-mail text, to space the appending data which embedded digital watermarking, and to create an entering E-mail, The electronic mail server equipment 20 which has a transmitting means 25 to space and to transmit an entering E-mail to another electronic mail server equipment by the usual delivery method, A receiving means 64 to receive contents data from the E-mail user equipment 50 of the receiving side which spaced and received the entering E-mail through electronic mail server equipment 40, When digital watermarking is detected from contents data and digital watermarking is detected, it has digital-watermarking detection equipment 60 which has a digital-watermarking detection means 61 to output the information currently embedded as information about unjust transmission.
[0012] A means by which this invention (claim 5) acquires the message ID which shows an E-mail to a meaning from this E-mail in electronic mail server equipment 10, Have further a means to make message ID and header information a group and to register with a header information database, and it sets for the digital-watermarking embedded means 23. It sets to digital-watermarking detection equipment 60 including the means which embeds message ID as digital watermarking in appending data using digital-watermarking technology. It considers that the information outputted by the digital-watermarking detection means 61 is message ID, and a means to acquire the E-mail which corresponds out of a header information database is included.
[0013] In another electronic mail server equipment with which an E-mail is transmitted to this invention (claim 6) from electronic mail server equipment A means to receive the E-mail where digital watermarking was embedded from electronic mail server equipment, A means to decompose an E-mail into the E-mail text and appending data, and a means to acquire the header information containing the destination e-mail address described by the header unit of an E-mail, When a means to detect digital watermarking from appending data, and detection of digital watermarking are successful It has a means to check the justification of an E-mail using a consistency check or the predetermined conditions of the destination e-mail address described by the destination e-mail address currently embedded and header information, and a means to perform processing for preventing injustice when justification cannot be checked.
[0014] this invention (claim 7) can be set to the contents protection system for preventing unjust distribution of contents in the case of the contents distribution using the network communication containing an E-mail. The appending data decomposition process which is the contents protection program which electronic mail server equipment performs, and decomposes into the E-mail text and appending data the E-mail sent from E-mail user equipment, The transmitting agency e-mail address described by the header unit of an E-mail, a destination e-mail address, a title, and the header information acquisition process of extracting the header information containing dispatch time, The digital-watermarking embedded process which embeds digital watermarking for header information in appending data using digital-watermarking technology, It has the appending data-coupling process which combines with the E-mail text, spaces the appending data which embedded digital watermarking, and creates an entering E-mail, and the transmitting process which spaces and transmits an entering E-mail to another electronic mail server equipment by the usual delivery method.
[0015] this invention (claim 8) has further the process which acquires the message ID which shows an E-mail to a meaning, and the process which makes message ID and

header information a group and is registered into a header information database, and includes the process which uses digital-watermarking technology and embeds message ID in appending data instead of header information in a digital-watermarking embedded process.

[0016] this invention (claim 9) can be set to the contents protection system for preventing unjust distribution of contents in the case of the contents distribution using the network communication containing an E-mail. The process which receives the E-mail where it is the contents protection program which electronic mail server equipment performs, and digital watermarking was embedded from other electronic mail server equipments, The process which decomposes an E-mail into the E-mail text and appending data, and the process which acquires the header information containing the destination e-mail address described by the header unit of an E-mail, When the process which detects digital watermarking from appending data, and detection of digital watermarking are successful The consistency check of the destination e-mail address described by the destination e-mail address currently embedded and header information Or it has the process which checks the justification of an E-mail using predetermined conditions, and the process which performs processing for preventing injustice when justification cannot be checked.

[0017] this invention (claim 10) can be set to the contents protection system for preventing unjust distribution of contents in the case of the contents distribution using the network communication containing an E-mail. Are the contents protection program which digital-watermarking detection equipment performs, and electronic mail server equipment is minded. The receiving process which receives contents data from the E-mail user equipment of the receiving side which spaced and received the entering E-mail, The digital-watermarking detection process of detecting digital watermarking from contents data, and when digital watermarking is detected When the header information currently embedded as digital watermarking is outputted as a log and is not able to be detected with the location information on contents data as information about unjust transmission, it has the output process which outputs the information showing detection failure as a log.

[0018] In an output process, this invention (claim 11) includes the process which acquires a corresponding E-mail from the header information database on the electronic mail server equipment message ID and the header information of an E-mail are registered by making it a group based on this message ID, when the information currently embedded as digital watermarking is message ID.

[0019] this invention (claim 12) can be set to the contents protection system for preventing unjust distribution of contents in the case of the contents distribution using the network communication containing an E-mail. The appending data decomposition process which is the storage which stored the contents protection program which electronic mail server equipment performs, and decomposes into the E-mail text and appending data the E-mail sent from E-mail user equipment, The transmitting agency e-mail address described by the header unit of an E-mail, a destination e-mail address, a title, and the header information acquisition process of extracting the header information containing dispatch time, The digital-watermarking embedded process which embeds digital watermarking for header information in appending data using digital-watermarking technology, It has the appending data-coupling process which combines with the E-mail text, spaces the appending data which embedded digital watermarking, and creates an entering E-mail, and the transmitting process which spaces and transmits an entering E-mail to another electronic mail server

equipment by the usual delivery method.
[0020] this invention (claim 13) has further the process which acquires the message ID which shows an E-mail to a meaning, and the process which makes message ID and header information a group and is registered into a header information database, and includes the process which uses digital-watermarking technology and embeds message ID in appending data instead of header information in a digital-watermarking embedded process.
[0021] this invention (claim 14) can be set to the contents protection system for preventing unjust distribution of contents in the case of the contents distribution using the network communication containing an E-mail. The process which receives the E-mail where it is the storage which stored the contents protection program which electronic mail server equipment performs, and digital watermarking was embedded from other electronic mail server equipments, The process which decomposes an E-mail into the E-mail text and appending data, and the process which acquires the header information containing the destination e-mail address described by the header unit of an E-mail, When the process which detects digital watermarking from appending data, and detection of digital watermarking are successful The consistency check of the destination e-mail address described by the destination e-mail address currently embedded and header information Or it has the process which checks the justification of an E-mail using predetermined conditions, and the process which performs processing for preventing injustice when justification cannot be checked.
[0022] this invention (claim 15) can be set to the contents protection system for preventing unjust distribution of contents in the case of the contents distribution using the network communication containing an E-mail. Are the storage which stored the contents protection program which digital-watermarking detection equipment performs, and electronic mail server equipment is minded. The receiving process which receives contents data from the E-mail user equipment of the receiving side which spaced and received the entering E-mail, The digital-watermarking detection process of detecting digital watermarking from contents data, and when digital watermarking is detected When the header information currently embedded as digital watermarking is outputted as a log and is not able to be detected with the location information on contents data as information about unjust transmission, it has the output process which outputs the information showing detection failure as a log.
[0023] In an output process, this invention (claim 16) includes the process which acquires a corresponding E-mail from the header information database on the electronic mail server equipment message ID and the header information of an E-mail are registered by making it a group based on this message ID, when the information currently embedded as digital watermarking is message ID.
[0024] As mentioned above, in this invention, when distributing contents as appending data of an E-mail, even if it carries out unjust distribution, those who performed injustice can pursue who it is, and the mental suppression of unjust distribution of them is attained by this by embedding the information which specifies a transmitting person and an addressee by digital-watermarking technology.
[0025] Moreover, in this invention, only the user specified by the copyright person will arrive in an E-mail, and contents data become possible [actually making unjust distribution impossible].
[0026]
[Embodiments of the Invention] Hereafter, the form of operation of this invention is explained with a drawing.

[0027] [Form of the 1st operation] drawing 3 shows the composition of the contents protection system in the form of operation of the 1st of this invention.
[0028] The electronic mail server equipment 40 by which the system shown in this drawing is connected to the networks 30, such as the Internet, and which delivers the usual E-mail, The electronic mail server equipment 20 with a digital-watermarking embedded function which has a digital-watermarking embedded function, and two or more E-mail user equipments 10 connected to electronic mail server equipment 20, It consists of digital-watermarking detection equipment 60 which detects digital watermarking from there in search of the contents data which include WWW (World Wide Web) etc., and are distributing and circulating on a network 30, and E-mail user equipment 50 connected to electronic mail server equipment 40.
[0029] In addition, in the above-mentioned composition, E-mail user equipment 10 is made into a transmitting side, and E-mail user equipment 50 is explained as a receiving side.
[0030] Next, operation in the above-mentioned composition is explained.
[0031] Drawing 4 is the sequence chart of processing of the contents protection system in the form of operation of the 1st of this invention.
[0032] Step 101 Transmitting-side side E-mail user equipment 10 creates an E-mail, and transmits it to electronic mail server equipment 20 with an E-mail embedded function.
[0033] Step 102 The electronic mail server equipment 20 with an E-mail embedded function uses for and embeds digital-watermarking technology to the contents data appended to the E-mail in the header information of the E-mail which received.
[0034] Step 103 The electronic mail server equipment 20 with an E-mail embedded function is spaced, delivers an entering E-mail with the usual mail delivery procedure, and transmits it to the electronic mail server equipment 40 which has managed the destination user.
[0035] Step 104 The E-mail of entering [space] reaches a destination user's E-mail user equipment 50. So far, it is exchange processing by the E-mail. Then, an addressee can acquire the contents data which spaced and were transmitted to entering mail.
[0036] Hereafter, operation of an about is explained when unjust distribution by the addressee is performed.
[0037] Step 105 From the E-mail user equipment 50 of an addressee, it spaces and distribution and circulation of entering contents data are done using WWW etc.
[0038] Step 106 Digital-watermarking detection equipment 60 acquires the contents data for detection by WWW page search etc.
[0039] Step 107 Digital-watermarking detection equipment 60 specifies the user who performed unjust distribution from the header information currently embedded, when the digital-watermarking detection from the contents data for detection is able to be tried and detected.
[0040] Next, above-mentioned composition and above-mentioned processing of electronic mail server equipment 20 with a digital-watermarking embedded function are explained.
[0041] Drawing 5 shows the composition of the electronic mail server equipment with a digital-watermarking embedded function in the form of operation of the 1st of this invention.
[0042] The electronic mail server equipment 20 with a digital-watermarking embedded function is the appending data decomposition section 21, the header

information acquisition section 22, the digital-watermarking embedding part 23, the appending data-coupling section 24, and SMTP (Simple Mail Transfer Protocol) that is the function of usual electronic mail server equipment. It consists of the SMTP processing sections 25 with the function as server equipment.
[0043] Drawing 6 is the flow chart of processing of the electronic mail server equipment with a digital-watermarking embedded function in the gestalt of operation of the 1st of this invention.
[0044] Electronic mail server equipment 20 will decompose an E-mail into the E-mail text and appending data in the appending data decomposition section 21 first, if the E-mail created by E-mail user equipment 10 is received (Step 201) (Step 202).
[0045] Next, in the header information acquisition section 22, header information is acquired from the E-mail text (Step 203). Header information is arbitrary combination, such as sender information, destination information, a title, and dispatch time.
[0046] Next, in the digital-watermarking embedded processing section 23, into appending data, digital-watermarking technology is used, and header information is embedded, and is spaced, and entering appending data are created. Here, when it spaces by performing digital-watermarking **** about all appending data and entering appending data are created, it spaces with (Step 204, Yes), and the E-mail text, and entering appending data are again combined in the appending data-coupling section 24 (Step 206), and the usual mail processing is performed in the SMTP processing section 25 (Step 207). When digital-watermarking **** about all appending data is not completed, (Step 204, No), and header information are embedded as digital watermarking to appending data, and it shifts to Step 204 (Step 205).
[0047] Next, above-mentioned composition and above-mentioned processing of digital-watermarking detection equipment 60 are explained.
[0048] Drawing 7 shows the composition of the digital-watermarking detection equipment in the gestalt of operation of the 1st of this invention. The digital-watermarking detection equipment 60 shown in this drawing consists of a digital-watermarking detecting element 61, the detection result logging section 62, and the log data base 63.
[0049] Drawing 8 is the flow chart of processing of the digital-watermarking detection equipment in the gestalt of operation of the 1st of this invention.
[0050] Digital-watermarking detection equipment 60 considers the location information on contents data and its contents data as an input (Step 301). As location information, URL (Uniform Resource Locator) etc. is raised, for example. Digital-watermarking detection equipment 60 acquires contents from WWW etc. one after another, and detects digital watermarking (Step 302). When detection of digital watermarking goes wrong, a detection result is created for the information showing (Step 303, No), and detection failure (Step 304). When it succeeds in detection of digital watermarking, based on (Step 303, Yes), and the header information currently embedded, a detection result is operated orthopedically and a detection result is created (Step 305).
[0051] The detection result created by the above is outputted to the log data base 63 as a log in the detection result logging section 62 (Step 306).
[0052] It turns out when the contents data concerned were delivered by someone and **** by the E-mail (the header information which should be embedded according to whether he wants what information to know is determined), and, thereby, the source information on the contents data by which unjust distribution was carried out etc. can be acquired from the outputted log data.

[0053] When the contents data which the addressee of an E-mail received by embedding the header information of an E-mail as digital watermarking in contents data when distributing contents data using an E-mail are distributed unjustly according to the gestalt of the 1st operation of the above, an unjust distribution person can be specified by detecting digital watermarking from the distributed contents data. The unjust distribution by the E-mail addressee can be mentally inhibited by this.
[0054] Moreover, the user who transmitted the E-mail can also specify by referring to the transmitting person address in header information, and the suppression effect over the contents distribution using the E-mail can also be realized.
[0055] Moreover, although the digital-watermarking embedded function needed to be included in a contents transmitting person's equipment and the installation work took time and effort in the usual contents protection system using digital-watermarking technology, change of what cannot add to the user equipment which transmits contents using mail server equipment, either, but it can apply easily to it by including a digital-watermarking function in mail server equipment with the gestalt of this operation.
[0056] The form of [form of the 2nd operation] book operation explains the object of digital watermarking about the example using not header information but message ID.
[0057] Except for the point of explaining below with the form of this operation, it is the same as that of the form of the 1st operation of the above-mentioned.
[0058] Drawing 9 is the sequence chart of processing of the contents protection system in the form of operation of the 2nd of this invention.
[0059] In the processing shown in this drawing, a different point from operation of drawing 4 is as follows.
[0060] In Step 402, the electronic mail server equipment 20 with a digital-watermarking embedded function embeds the message ID given to the E-mail to the contents data appended to the E-mail. Simultaneously, the header information of message ID and an E-mail is registered into the header information database in electronic mail server equipment 20 with a digital-watermarking embedded function.
[0061] In Step 407, when the digital-watermarking detection from the contents data for detection is able to be tried and detected, digital-watermarking detection equipment 60 is acquiring the message ID currently embedded and corresponding header information from a header information database, and specifies the user who performed unjust distribution.
[0062] Next, the composition of above electronic mail server equipment 20 with a digital-watermarking embedded function is explained.
[0063] Drawing 10 shows the composition of the electronic mail server equipment with a digital-watermarking embedded function in the form of operation of the 2nd of this invention.
[0064] In addition to the appending data decomposition section 21 shown in drawing 5 , the header information acquisition section 22, the digital-watermarking embedding part 23, the appending data-coupling section 24, and the SMTP processing section 25, the electronic mail server equipment 20 with a digital-watermarking embedded function shown in this drawing consists of the message ID acquisition section 26 and a header information database 27.
[0065] Drawing 11 is the flow chart of processing of the electronic mail server equipment with a digital-watermarking embedded function in the form of operation of the 2nd of this invention.
[0066] the E-mail by which electronic mail server equipment 20 was created with E-mail user equipment 10 -- receiving (Step 401) -- in the appending data

decomposition section 21, an E-mail is first decomposed into the E-mail text and appending data (Step 402)
[0067] Next, in the message ID acquisition section 26, message ID is acquired from the E-mail text (Step 403). Message ID is an identifier for specifying the E-mail concerned as a meaning usually given by E-mail user equipment 10 or the electronic mail server equipment 20 which received the E-mail from E-mail user equipment 10. With the form of this operation, when message ID is given by the E-mail user equipment 10 side, message ID is read from an E-mail as mentioned above, and in giving message ID by the electronic mail server equipment 20 side, electronic mail server equipment 20 generates the message ID showing the received E-mail itself, and embeds this by the digital-watermarking embedding part 23. here -- digital-watermarking embedded -- when **** is being performed for digital watermarking about no possible appending data, (Step 404, No), and message ID are embedded as digital watermarking to appending data, and it shifts to Step 404 (Step 405) When digital-watermarking embedding is performed to all appending data, header information is read from the E-mail text in (Step 404, Yes), and the header information acquisition section 22 (Step 406), and it is made message ID and a group, and registers with the header information database 27 (Step 407). It spaces with the E-mail text, entering appending data are again combined in the appending data-coupling section 24 (Step 408), and the usual mail processing is performed in the SMTP processing section 25 (Step 409).
[0068] Next, the digital-watermarking detection equipment in the form of this operation is explained.
[0069] Drawing 12 shows the composition of the digital-watermarking detection equipment in the form of operation of the 2nd of this invention. The digital-watermarking detection equipment shown in this drawing is the same as that of the composition shown in drawing 7 in the form of the 1st operation of the above-mentioned. In the form of this operation, differing from the form of the 1st operation of the above-mentioned is only the point that the information acquired by digital-watermarking detection processing is not header information but message ID. Digital-watermarking detection equipment 60 makes this message ID and location information a group, and outputs them to the log data base 63.
[0070] Drawing 13 is drawing for explaining the inaccurate user specification procedure in the form of operation of the 3rd of this invention.
[0071] Message ID and header information are accumulated, and in the log data base 63, message ID and location information become a group, respectively, and are accumulated at the header information database 27 of electronic mail server equipment 20 with a digital-watermarking embedding function. Matching of header information and location information is performed by collating the record in these two databases by message ID. In this case, for example, ISP which has managed the header information database, message ID may be sent to the manager of digital-watermarking detection equipment 60, it may match in the form of "Wanting you to teach the log of the location information on contents that this message ID was embedded", may send message ID to the manager of digital-watermarking detection equipment 60 to ISP conversely, and may match in the form of "Wanting you to teach the header information of mail expressed with this message ID."
[0072] Drawing 14 is the flow chart of processing of the digital-watermarking detection equipment in the form of operation of the 2nd of this invention.
[0073] The digital-watermarking detecting element 61 inputs contents data and the

location information on contents (Step 501), and digital watermarking is detected from contents data (Step 502). In not succeeding in detection of digital watermarking (Step 503, No), it creates the purport which was not able to be detected as a detection result (Step 504). When you succeed, let message ID currently embedded as a watermark be a detection result (Step 505). The detection result logging section 62 makes a detection result and location information a group, and outputs a log to the log data base 63 (Step 506).

[0074] According to the gestalt of this above-mentioned operation, the amount of information which should generally be embedded as digital watermarking rather than all header information compared with the gestalt of the 1st operation of the above-mentioned since the direction of message ID has little amount of information is reducible, and further, in digital-watermarking technology, since embedding amount of information and resistance (the difficulty of disappearing) have the relation of a trade-off, the resistance of digital watermarking can be raised.

[0075] Moreover, it is thought that there are many gestalten from which the subject which employs mail server equipment, and the subject which employs the digital-watermarking detection equipment which reads digital watermarking in the contents on a network differ as a gestalt of employment of this invention. In this case, the employment subject of mail server equipment requests the digital-watermarking detection equipment employment subject which is creating the log of digital-watermarking detection at any time, saying "I want you to teach the location information (URL etc.) on contents that the message ID of OO watch was embedded", and a digital-watermarking detection equipment employment subject offers location information in response to this.

[0076] The information embedded with the gestalt of this operation at digital watermarking is message ID, and since the header information corresponding to message ID is in a mail server equipment side, header information is not obtained in a digital-watermarking detection equipment side.

[0077] Generally, the information concerning the privacy of users, such as an E-mail transmitting person and a destination user, is included in header information. Although it is not desirable, according to the gestalt of this operation, as above-mentioned, it can solve this problem that these information gets across to a digital-watermarking detection equipment employment subject unrelated to a user, and it is useful also to privacy protection.

[0078] The gestalt of [gestalt of the 3rd operation] book operation explains the case where a digital-watermarking detection function is given to electronic mail server equipment.

[0079] The gestalt of this operation performs the same composition as the gestalt of the 1st operation of the above-mentioned, and operation except for the point of explaining below.

[0080] Drawing 15 shows the composition of the contents protection system in the gestalt of operation of the 3rd of this invention. The system shown in this drawing consists of electronic mail server equipment 20 with a digital-watermarking embedded function which is connected to the networks 30, such as the Internet, and which has a digital-watermarking embedded function, electronic mail server equipment 70 with a digital-watermarking detection function which has a digital-watermarking detection function, and two or more E-mail user equipments 10 and 50 connected to electronic mail server equipment 20 with a digital-watermarking embedded function.

[0081] Drawing 16 is the sequence chart of processing of the contents protection

system in the form of operation of the 3rd of this invention.
[0082] Step 601 An E-mail is created with transmitting person side E-mail user equipment 10, and it is transmitted to electronic mail server equipment 20 with an E-mail embedded function.
[0083] Step 602 The electronic mail server equipment 20 with an E-mail embedded function uses for and embeds digital-watermarking technology at contents DEA appended to the E-mail in the header information containing the destination address of the E-mail which received.
[0084] Step 603 The electronic mail server equipment 20 with an E-mail embedded function is spaced, delivers an entering E-mail with the usual mail delivery procedure, and transmits it to the electronic mail server equipment 70 with a digital-watermarking detection function which has managed the destination user.
[0085] Step 604 The electronic mail server equipment 70 with a digital-watermarking detection function checks coincidence of the destination address of the destination address currently embedded and the header of the E-mail text, when detection of digital watermarking is tried from the received appending data which space and are appended to the entering E-mail and it succeeds in detection. When in agreement, it shifts to Step 605, and inharmonious processing is performed when not in agreement. As inharmonious processing, processing of sending the warning [space and / sender / of an entering E-mail / "contents data tended to be appended to the destination which is not permitted and it was going to carry out mail distribution"] mail concerned can be considered, for example.
[0086] Step 605 If in agreement, it will distribute to the E-mail user equipment 50 through which it spaces as usual and which a destination address shows an entering E-mail.
[0087] The electronic mail server equipment 20 with a digital-watermarking embedded function in the form of this operation embeds the destination address information on an E-mail as indispensable as header information embedded in appending data.
[0088] Drawing 17 shows the composition of the electronic mail server equipment with a digital-watermarking detection function in the form of operation of the 3rd of this invention.
[0089] The electronic mail server equipment 70 with a digital-watermarking detection function shown in this drawing consists of the STMP processing section 71, the appending data decomposition section 72, the header information acquisition section 73, the digital-watermarking detecting element 74, the coincidence check section 75, the inharmonious processing section 76, and the E-mail delivery section 77.
[0090] Drawing 18 is the flow chart of processing of the electronic mail server equipment with a digital-watermarking detection function in the form of operation of the 3rd of this invention.
[0091] First, the electronic mail server equipment 70 with a digital-watermarking detection function spaces by performing the usual E-mail reception according to an SMTP protocol in the SMTP processing section 71, and inputs an entering E-mail (Step 701).
[0092] Next, in the appending data decomposition section 72, it spaces and an entering E-mail is decomposed into the E-mail text and appending data (Step 702). Next, in the header information acquisition section 73, destination mail address information is acquired from the header of the E-mail text (Step 703).
[0093] Next, in the digital-watermarking detecting element 74, the digital-

watermarking detection from appending data is tried. Under the present circumstances, when digital watermarking is not able to be detected from appending data, an E-mail is delivered to the E-mail user equipment 50 which a destination address shows as (Step 704, No), and usual (Step 707). It investigates whether when it succeeds in detection of digital watermarking (Step 704, Yes), the destination address information currently embedded and the destination address information read in the header are in agreement in the coincidence check section 75, and when in agreement, (Step 705, Yes), and an E-mail are delivered to the E-mail user equipment 50 which a destination address shows (Step 707). In not being in agreement, when inharmonious, in (Step 705, No), and the inharmonious processing section 76, it performs sending of the processing to perform, for example, the above-mentioned warning mail, etc. (Step 706).

[0094] According to the form of this above-mentioned operation, using electronic mail server equipment 20 with a digital-watermarking embedded function, a regular contents distribution person embeds digital watermarking, and delivers the destination of contents data, and when it is destination user type electronic mail server equipment 70 with an electronic mail server equipment ********** detection function of the contents data concerned, contents distribution can be performed satisfactory.

[0095] Furthermore, if the destination user of the contents data concerned is going to do unjust distribution of the contents data at another user, when the electronic mail server equipment by the side of another user is electronic mail server equipment with a digital-watermarking detection function, contents distributing becomes impossible and unjust distribution cannot be performed. Without adding change for such unjust distribution prevention to the E-mail user equipment by the side of a user entirely, it can realize only by changing the equipment by the side of ISP which employs electronic mail server equipment, and compatibility with the present employment is high. Moreover, if there is much ISP it is considered that wants to avoid a user's injustice which oneself manages and electronic mail server equipment with a digital-watermarking detection function is used by each ISP, the unjust distribution prevention by this invention can improve a function further. Moreover, with the form of this operation, although contents protection is aimed at by conducting coincidence inspection about a destination e-mail address, different contents protection "until can be delivered when on what [, what / month / what]" is also easily realizable using another information, for example, time information.

[0096] Moreover, or it installs in the computer which builds the component of the electronic mail server equipment in the form of the above-mentioned operation, and digital-watermarking detection equipment as a program, and is used as electronic mail server equipment and digital-watermarking detection equipment, it is possible to make it circulate through a network.

[0097] Moreover, this invention is easily realizable by installing, in case the built program is stored in portable storages, such as a hard disk drive unit connected to the computer used as electronic mail server equipment and digital-watermarking detection equipment, and a floppy (registered trademark) disk, CD-ROM, and this invention is carried out.

[0098]

[Effect of the Invention] As mentioned above, according to this invention, by embedding the information which specifies a transmitting person and an addressee by digital-watermarking technology, when distributing contents as appending data of an E-mail, even if a user does unjust distribution, it can pursue who those who performed injustice are.

[0099] Moreover, mental suppression of unjust distribution of a user is realizable with this.
[0100] Furthermore, contents data will reach only the user specified by the copyright person in an E-mail, and can actually make unjust distribution impossible.

[Translation done.]

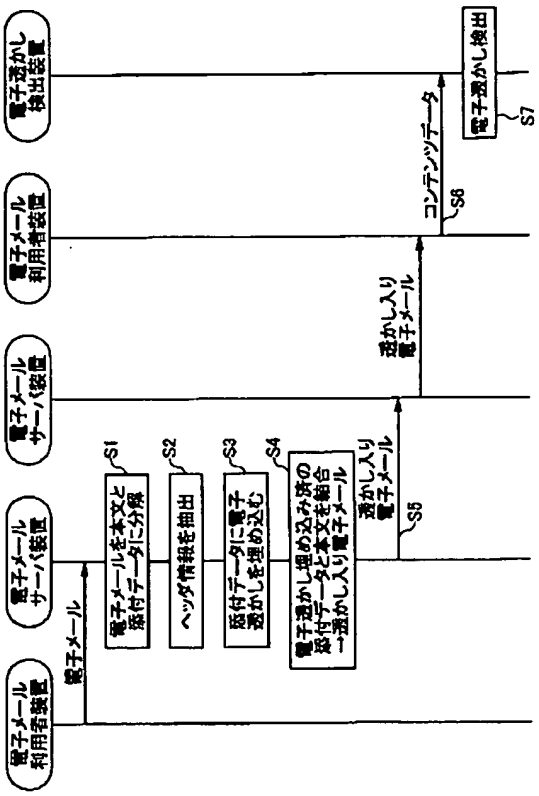
* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

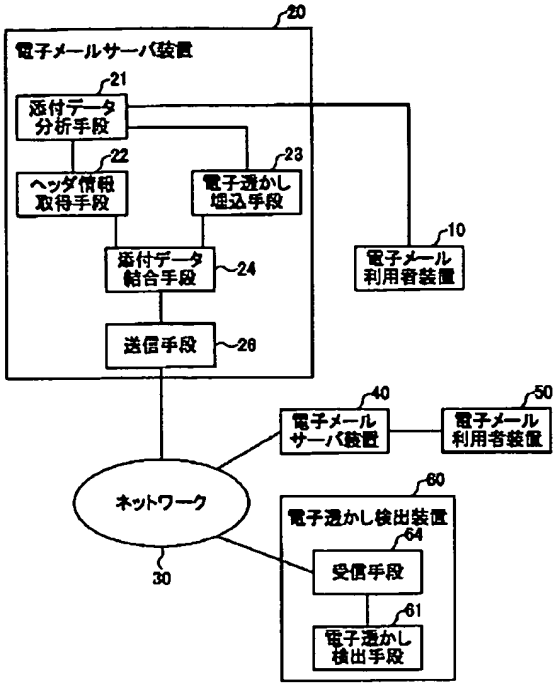
[Drawing 1]

本発明の原理構成図



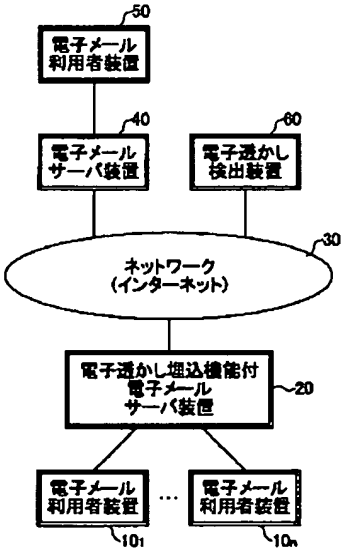
[Drawing 2]

本発明の原理構成図



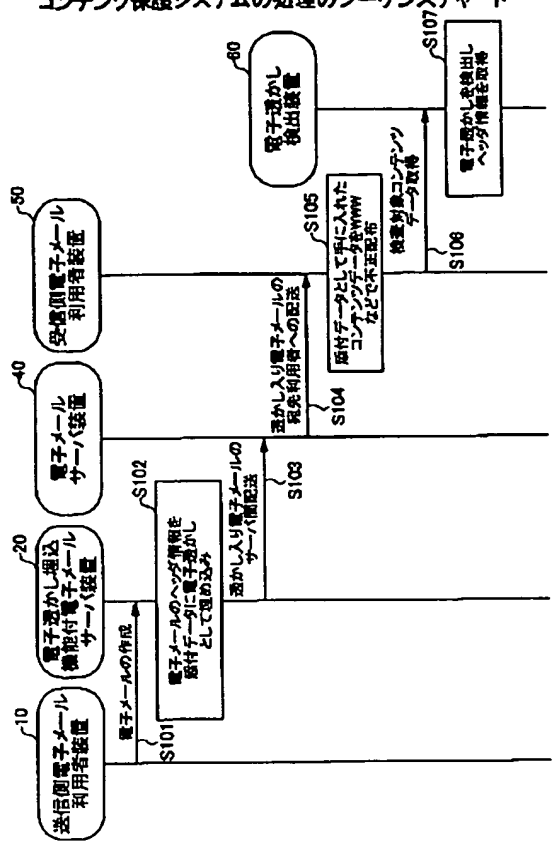
[Drawing 3]

本発明の第1の実施の形態におけるコンテンツ保護システムの構成を示す図



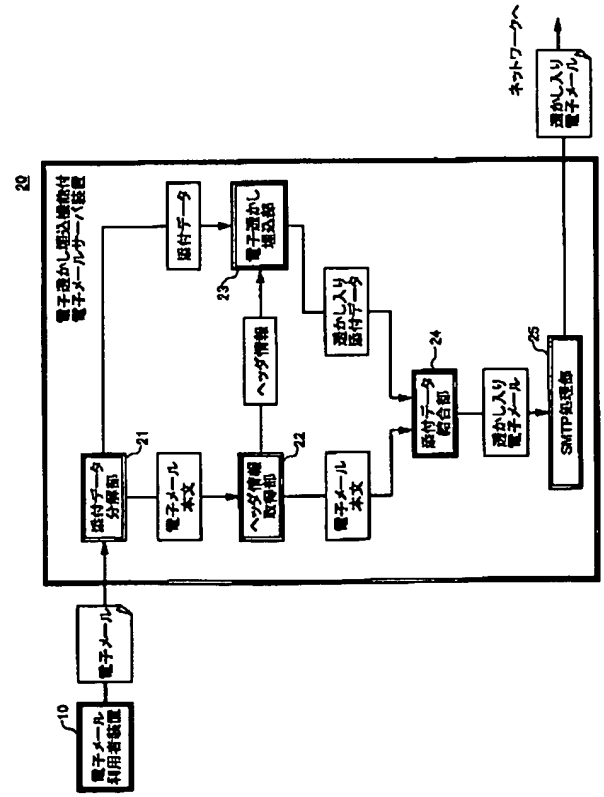
[Drawing 4]

本発明の第1の実施の形態における
コンテンツ保護システムの処理のシーケンスチャート



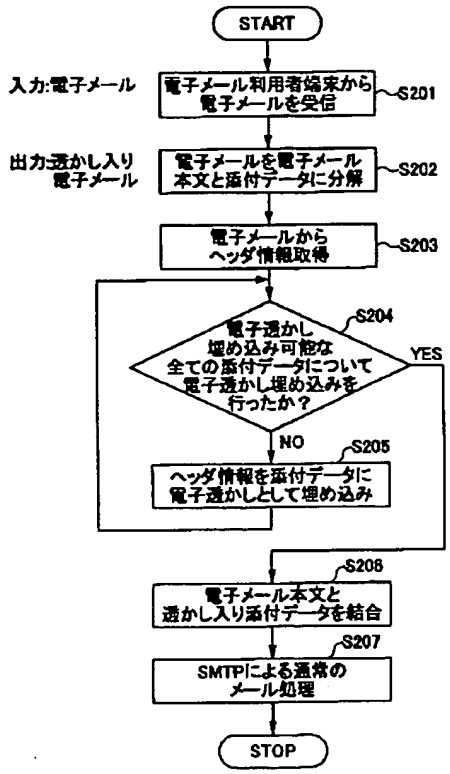
[Drawing 5]

本発明の第1の実施の形態における電子透かし埋込機能付
電子メールサーバ装置の構成図



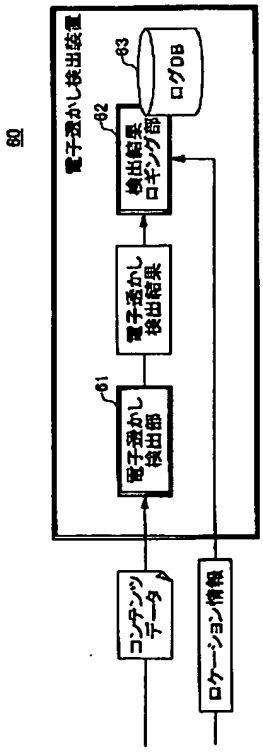
[Drawing 6]

本発明の第1の実施の形態における電子透かし埋込機能付電子メールサーバ装置の処理のフローチャート



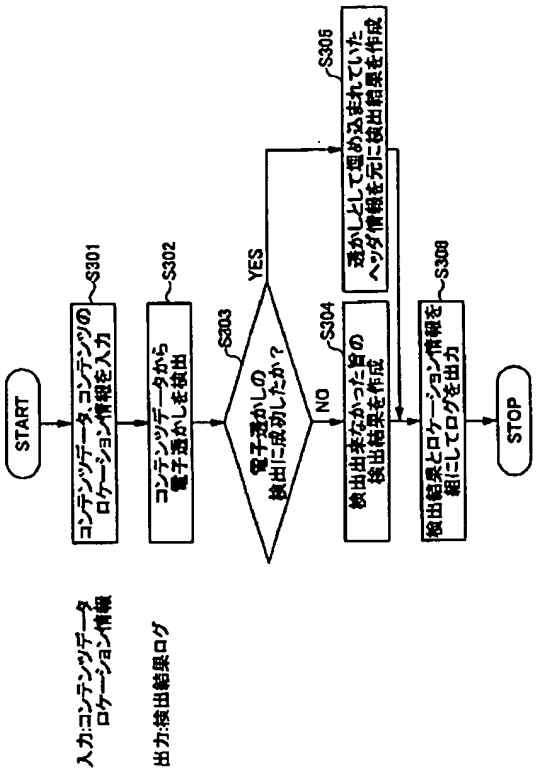
[Drawing 7]

本発明の第1の実施の形態における電子透かし検出装置の構成図



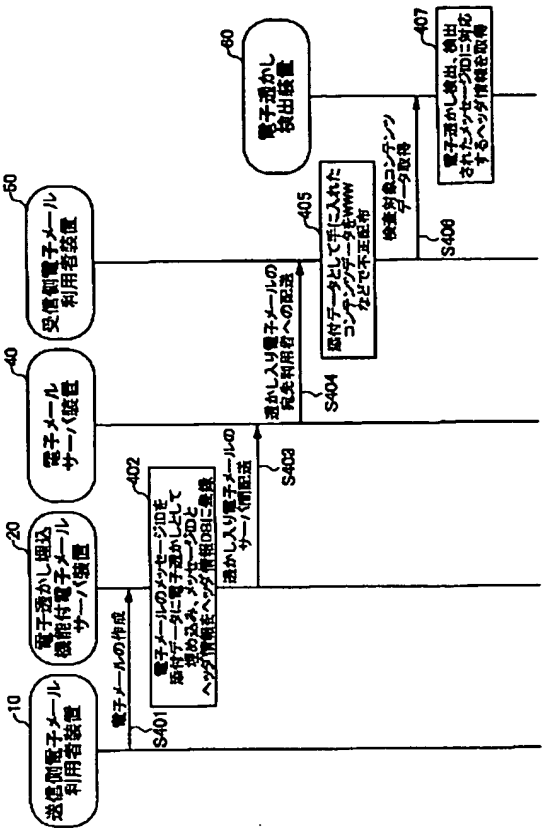
[Drawing 8]

本発明の第1実施の形態における
電子透かし検出装置の処理のフローチャート



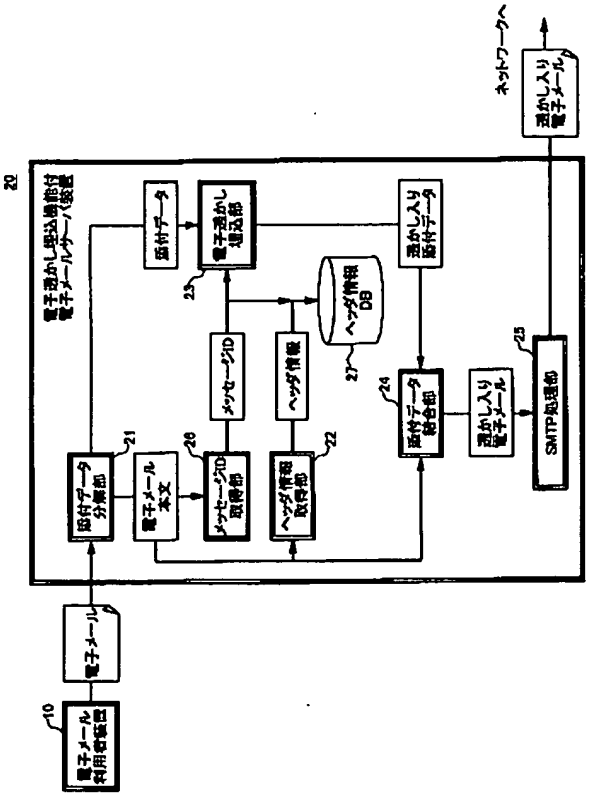
[Drawing 9]

本発明の第2の実施の形態における
コンテンツ保護システムの処理のシーケンスチャート



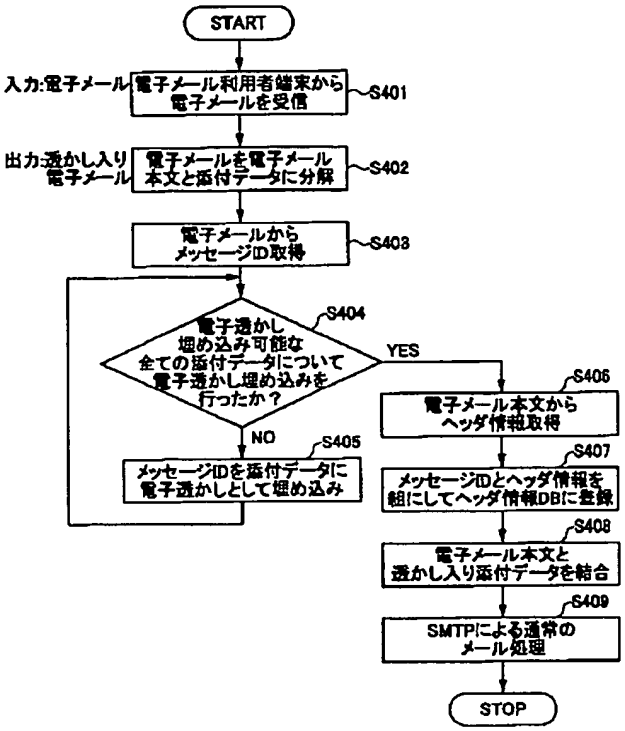
[Drawing 10]

本発明の第2の実施の形態における電子透かし埋込機能付
電子メールサーバ装置の構成図



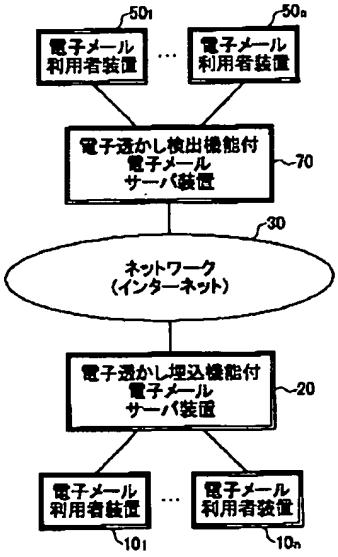
[Drawing 11]

本発明の第2の実施の形態における電子透かし埋込機能付電子メールサーバ装置の処理のフローチャート



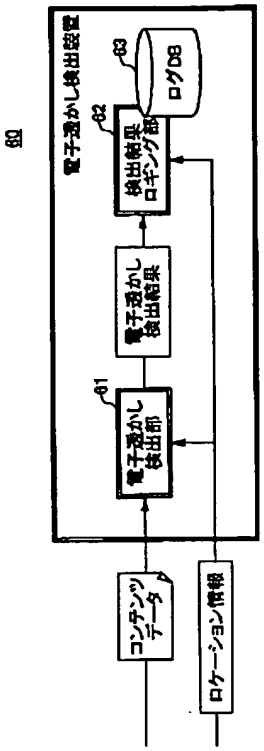
[Drawing 15]

本発明の第3の実施の形態におけるコンテンツ保護システムの構成を示す図



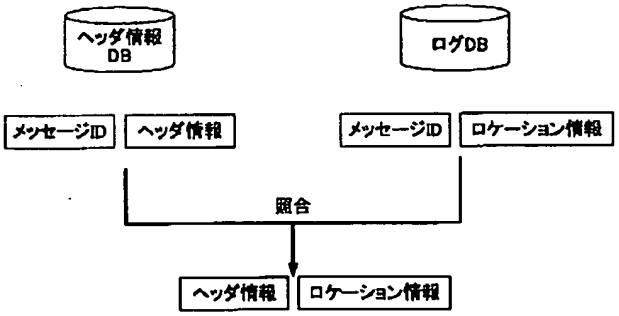
[Drawing 12]

本発明の第2の実施の形態における電子透かし検出装置の構成図



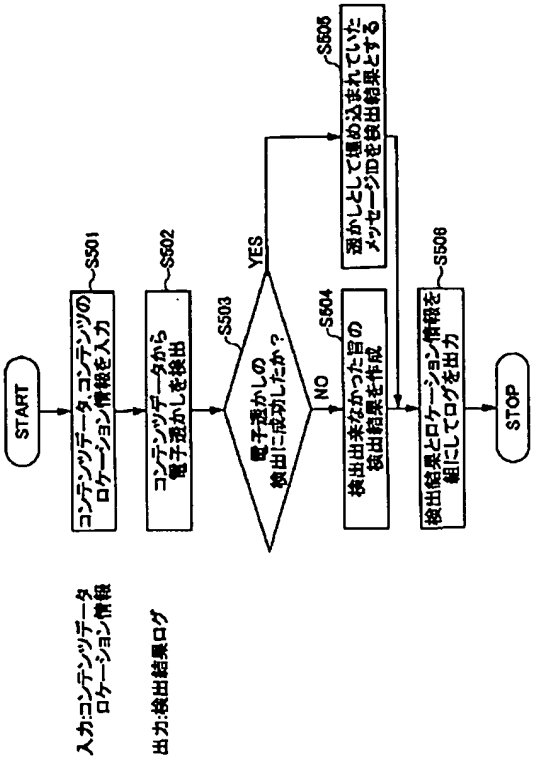
[Drawing 13]

本発明の第2の実施の形態における
不正利用者特定手順を説明する図



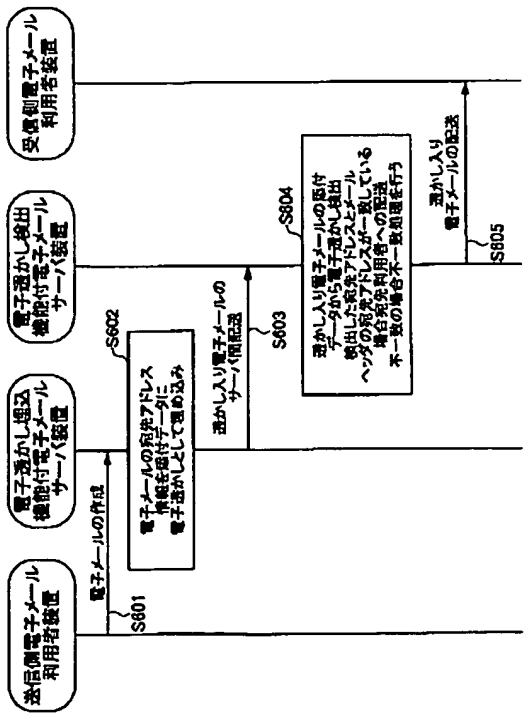
[Drawing 14]

本発明の第2実施の形態における
電子透かし検出装置の処理のフローチャート



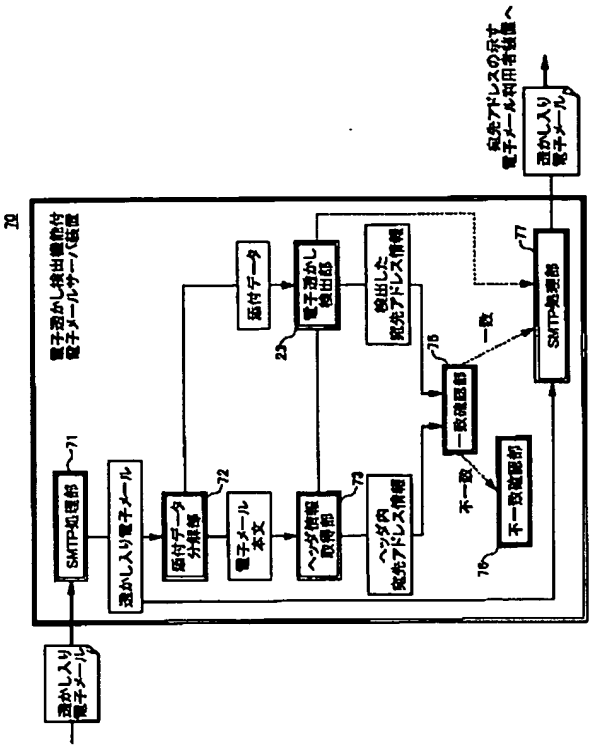
[Drawing 16]

本発明の第3の実施の形態における
コンテンツ保護システムの処理のシーケンスチャート



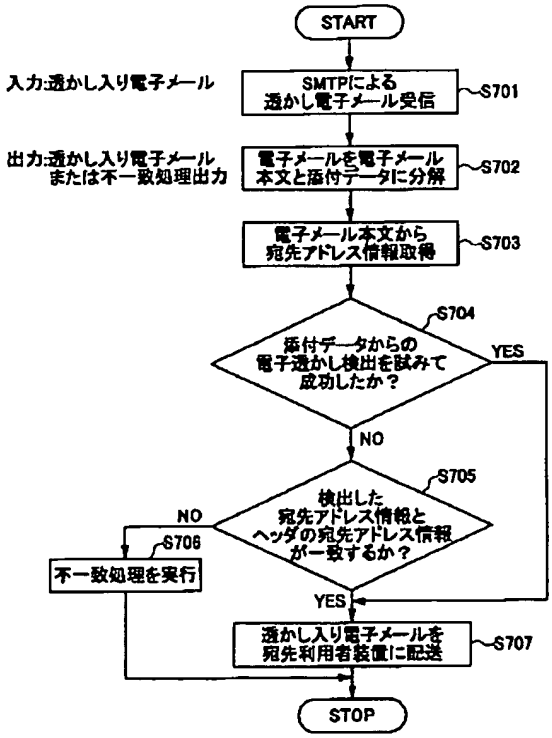
[Drawing 17]

本発明の第3の実施の形態における電子透かし検出機能付
電子メールサーバ装置の構成図



[Drawing 18]

本発明の第3の実施の形態における電子透かし検出機能付
電子メールサーバ装置の処理のフローチャート



[Translation done.]